Oracle Key Vault 21.15

nShield® HSM Integration Guide

2026-09-23

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
    1.1. Product configurations . . . 1
    1.2. Supported nShield hardware and software versions . . . 1
    1.3. Supported nShield functionality . . . 2
    1.4. Requirements . . . 2
    1.5. More information . . . 3
2. Procedures . . . 5
    2.1. Install HSM client software on the Key Vault server . . . 5
    2.2. Enroll Key Vault as a client of the HSM . . . 6
    2.3. Enable HSM mode in Key Vault . . . 9
    2.4. Configure an HSM for a multi-master cluster . . . 12
    2.5. Reverse migration operations to a local wallet . . . 18
    2.6. Configure backup of the Key Vault server in HSM mode . . . 20
    2.7. Restore from a Key Vault backup in HSM mode . . . 21
    2.8. Restart or restore in HSM mode using nShield Remote Administration . . . 22
3. Additional resources and related products . . . 23
    3.1. nShield HSMs . . . 23
    3.2. nShield as a Service . . . 23
    3.3. Entrust products . . . 23
    3.4. nShield product documentation . . . 23

Chapter 1. Introduction

This guide describes how to integrate Entrust nShield Hardware Security Modules (HSMs) with Oracle Key Vault.

The HSM generates and stores a Root of Trust (RoT) that protects the security objects used by Oracle Key Vault to safeguard user keys and credentials. The HSM can be used in FIPS 140 Level 2 or Level 3 mode to meet compliance requirements.

Note that:

- Oracle Key Vault cluster nodes can connect to individual HSMs, share the same user account on one HSM, or have individual user accounts on one HSM.
- An existing Oracle Key Vault deployment can be migrated to use an HSM as a Root of Trust.
- Oracle Key Vault does not start if the RoT stored in the HSM is not available or if Oracle Key Vault cannot reach the HSM.
- To restart or restore Key Vault in HSM mode when Operator Card Set (OCS) protection is used, the OCS for the HSM must be in slot 0 of the HSM.

1.1. Product configurations

Entrust has successfully tested nShield HSM integration with Oracle Key Vault in the following configurations:

Product	Version
Oracle Key Vault	21.15
Security World Software	13.6.18

1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

1.2.1. Connect XC

Security World Software	Firmware	Image	OCS	Softcard	Module
13.6.18	12.72.4 (FIPS 140-2 certified)	13.6.18	✓	✓	✓

1.2.2. nShield 5c

Security World Software	Firmware	Image	OCS	Softcard	Module
13.6.18	13.4.5 (FIPS 140-3 certified)	13.6.18	✓	✓	✓

1.3. Supported nShield functionality

Feature	Support
Key generation	Yes
1-of-N Operator Card Set	Yes
FIPS 140 Level 3 support	Yes
Key management	Yes
k-of-N Operator Card Set	No
Common Criteria support	Yes
Key import	Yes
Softcards	Yes
Load sharing	Yes
Key recovery	Yes
Module-Only key	Yes
Fail over	Yes

1.4. Requirements

Before installing these products, read the associated documentation:

- For the nShield HSM: *Installation Guide* and *User Guide*.
- If nShield Remote Administration is to be used: *nShield Remote Administration User Guide*.
- Oracle Key Vault documentation (https://docs.oracle.com/en/database/oracle/key-vault).

In addition, the integration between nShield HSMs and Oracle Key Vault requires:

- A separate non-HSM machine on the network to use as the Remote File System for the HSM. The RFS machine can also be used as a client to the HSM, to allow presentation of Java Cards using nShield Remote Administration. See the *nShield Remote Administration User Guide*.
- PKCS #11 support in the HSM.
- A correct quorum for the Administrator Card Set (ACS).
- Operator Card Set (OCS), Softcard, or Module-Only protection.

  If OCS protection is to be used, a 1-of-N quorum must be used.

- Firewall configuration with usable ports:
  - 9004 for the HSM (hardserver).
  - 8200 for Key Vault.

Furthermore, the following design decisions impact how the HSM is installed and configured:

- Whether your Security World must comply with FIPS 140 Level 3 standards.

  If using FIPS 140 Level 3, it is advisable to create an OCS for FIPS authorization. The OCS can also provide key protection for the Vault master key. For information about limitations on FIPS authorization, see the *Installation Guide* for the nShield HSM.

- Whether to instantiate the Security World as recoverable or not.

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

1.5. More information

For more information about OS support, contact your Oracle Key Vault sales representative or Entrust nShield Support at https://nshieldsupport.entrust.com.

Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

Chapter 2. Procedures

The high-level procedure to install and configure one or more Oracle Key Vault servers with one or more nShield HSMs is as follows:

1. Install the required number of instances of Oracle Key Vault. For instructions, see the Oracle Key Vault documentation.
2. Install and configure the required number of HSMs and the Security World software, including setting up the Remote File System (RFS) or Remote Administration. For instructions, see the *Installation Guide* for your HSM.
    - nShield HSMs require a separate non-HSM machine on the network to use as the RFS. You must set up this machine and copy the nShield Security World Software files to it before you install the HSM client software on Oracle Key Vault servers.
    - All enrolled HSMs must be in the same Security World and must have access to the OCS in slot 0 if OCS-protection is used. If the HSM whose slot 0 is used is enrolled on each of the Key Vault servers, the Key Vault web user interface has access to all of the HSMs, as long as they are in the same Security World.
    - If a FIPS Level 3 world file is used, all enrolled HSMs must have access to an OCS for FIPS authorization.
    - If dynamic slots are to be used on the HSMs, set up Remote Administration and configure slot mapping.
3. Install the HSM client software on the Oracle Key Vault server(s).
4. Enroll the Key Vault server(s) as client(s) of the HSM(s).
5. Enable HSM mode in the Oracle Key Vault web user interface.
6. For a high-availability Oracle Key Vault environment, enroll your HSM and configure initialization of the HSM in each of the nodes.

2.1. Install HSM client software on the Key Vault server

Perform these steps on the Oracle Key Vault server. For a high-availability Oracle Key Vault environment, perform these steps on each Key Vault instance to be added to the cluster.

To install HSM client software on the Key Vault server:

1. Log in to the Oracle Key Vault server as the `support` user using SSH:

```
$ ssh support@<okv_instance>
<Enter the support user password when prompted>
```

2. Switch to root:

```
$ su root
```

3. Install the latest version of the Security World software as described in the *Installation Guide* for the HSM.

Entrust recommends that you uninstall any existing nShield software before installing the new nShield software.

4. Create the Security World as described in the *User Guide*, creating the ACS and OCS that you require.
5. As root on the Key Vault server, add the `nfast` group to the `oracle` user:

```
root# usermod -a -G nfast oracle
```

6. Switch to the `oracle` user and verify the installation:

```
root# su oracle
oracle$ PATH=/opt/nfast/bin:$PATH
oracle$ export PATH
oracle$ enquiry
```

The mode should say `operational` in the output. For example:

```
Server:
enquiry reply flags  none
enquiry reply level  Six
serial number        nnnn-nnnn-nnnn
mode                 operational
version              13.4.5
speed index          15843
```

7. Restart the Oracle Key Vault server for the group change to take effect.

To restart or restore Key Vault in HSM mode when OCS protection is used, the OCS for the HSM must be in slot 0 of the HSM.

8. As the `root` user, set firewall rules to enable port 9004 for the hardserver (the client process in the nShield Security World software that communicates with the HSM).

2.2. Enroll Key Vault as a client of the HSM

To enroll Key Vault as a client of the HSM:

1. Add the Key Vault server IP address to the client list on the HSM using the front panel or via an update to the Connect configuration file. For instructions, see the *User Guide* for your HSM.
    a. Select privileged on any port.
    b. For a high-availability Oracle Key Vault environment, add the IP addresses of all Key Vault servers to the client list on all HSMs.
2. Switch to the `oracle` user:

```
root# su oracle
oracle$ PATH=/opt/nfast/bin:$PATH
oracle$ export PATH
```

3. To obtain the ESN and keyhash for the `nethsmenroll` command in the next step, run the `anonkneti` command:

```
anonkneti <HSM IP address>
```

4. On the Key Vault server, enroll with the HSM:

```
oracle$ nethsmenroll --privileged <HSM IP address> <HSM ESN> <HSM keyhash>
```

5. Run the following command:

```
enquiry
```

   Verify that the HSM mode is operational and the hardware status is OK.

6. Configure TCP sockets:

```
oracle$ config-serverstartup --enable-tcp --enable-privileged-tcp
```

7. Switch to root and restart the hardserver:

```
oracle$ su root
root# /opt/nfast/sbin/init.d-ncipher restart
```

8. On the Remote File System machine, run the following command:

```
rfs-setup --gang-client --write-noauth <IP address of your Key Vault server>
```

9. If OCS protection is intended but the Security World has not been created yet, edit the `cardlist` file to enable Java Cards for use through dynamic slots. If the Security World

has been created with this RFS, this configuration is already enabled.

a. Go to the following directory on the RFS:

```
#/opt/nfast/kmdata/config
```

b. Open the `cardlist` file in a text editor.

c. Add an asterisk (*) to authorize all Java Cards for dynamic slots.

If only certain Java Cards are authorized for this use, list them by their serial number. For example:

```
4286005559064791
4286005559064792
4286005559064793
```

d. Copy the updated `cardlist` file from the RFS to all clients.

10. On the Key Vault server as the `oracle` user, run the following commands:

```
oracle$ rfs-sync --setup <IP address of Remote File System machine>
oracle$ rfs-sync --update
```

11. As the `root` user, create the `/opt/nfast/cknfastrc` configuration file for PKCS#11 variables. For information on these variables, see the *User Guide* for your HSM.

a. OCS protection.

If you are using OCS or Module protection, set `cknfastrc`:

```
CKNFAST_NO_ACCELERATOR_SLOTS=1
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=explicitness;tokenkeys;longterm;wrapping_crypt
```

b. Softcard Protection.

If you are using Softcard protection, then `CKNFAST_LOADSHARING` must be set. This is not supported alongside the Module-only Key protection settings.

```
CKNFAST_LOADSHARING=1
CKNFAST_NO_ACCELERATOR_SLOTS=1
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=explicitness;tokenkeys;longterm;wrapping_crypt
```

c. Module Protection.

If you are using Module-Only protection, set `cknfastrc`:

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=explicitness;tokenkeys;longterm;wrapping_crypt
```

```
CKNFAST_FAKE_ACCELERATOR_LOGIN=1
```

12. On the Key Vault Server, test PKCS#11 access as follows:

```
oracle$ /opt/nfast/bin/ckcheckinst
```

Select a slot number to run a library test. Various slots are displayed, depending on your configuration.

Example 1:

```
0 Fixed token "accelerator"
1 Operator card "OKV_OCS"
```

Example 2:

```
0  Operator card     "OKV_OCS"
1  Soft token        "OKV_Softcard"
```

Test execution:

```
Test                    Pass/Failed
----                    -----------

1 Generate RSA key pair   Pass
2 Generate DSA key pair   Pass
3 Encryption/Decryption   Pass
4 Signing/Verification    Pass

Deleting test keys         ok

PKCS#11 library test successful.
```

2.3. Enable HSM mode in Key Vault

After installing HSM software and enrolling Key Vault as an HSM client, you can enable HSM mode with nShield HSM(s) from the Key Vault web user interface. This will protect the Oracle Key Vault Root of Trust key with the HSM.

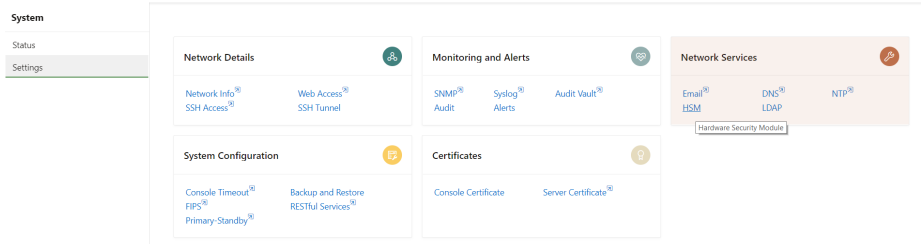
1. Log in to the Oracle Key Vault web user interface as a Key Administrator.

   The **Oracle Key Vault Home** page appears.

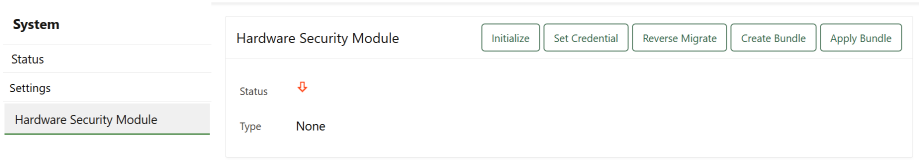
2. Select the **System** tab.

   The **Status** page appears.

3. Select **Settings** on the left menu.
4. Under **Network Services**, select **HSM**.



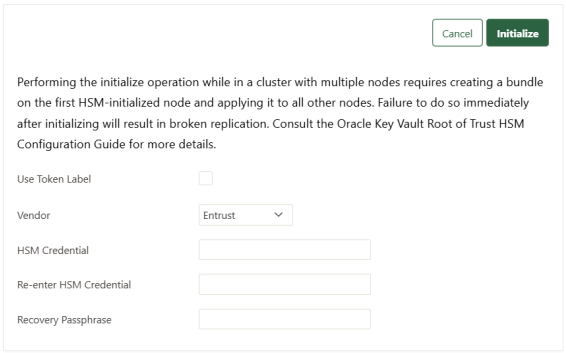
The **Hardware Security Module** page appears.



The red downward arrow shows the non-initialized **Status**. The **Type** field displays **None**.

5. Select **Initialize**.

   The **Initialize HSM** dialog appears.

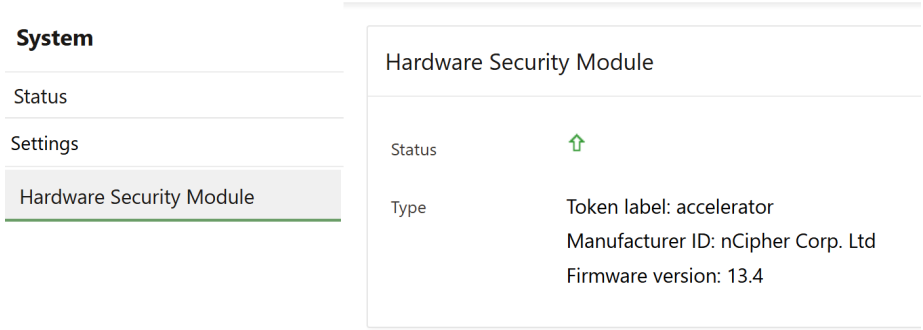


6. From the **Vendor** list, select **Entrust**.
7. Enter a password two times: first in **HSM Credential** and second in **Re-enter HSM Credential**.
   - If you are using OCS protection, then your OCS passphrase needs to be entered twice with your card presented in slot 0.
   - If you are using Softcard protection, then the Softcard passphrase needs to be entered twice.
   - If you are using Module-Only protection, enter a password that you set up for this credential check.

The password will be needed in the future, for example for reverse migration.

8. If using a FIPS Level 3 world file, have an OCS card mounted to provide FIPS authorization.
9. Make sure the `cknfastrc` file is set according to the type of protection being used.
10. Enter the recovery passphrase for Oracle Key Vault.
11. If you are using token labels, used for OCS protection and Softcards for instance, check the **Use Token Label** checkbox and enter the name of the token.
12. Select **Initialize**.

    At the end of a successful initialize operation, the **Hardware Security Module** page appears. The initialized **Status** is indicated by a green upward arrow. The **Type** field shows details of the HSM in use.



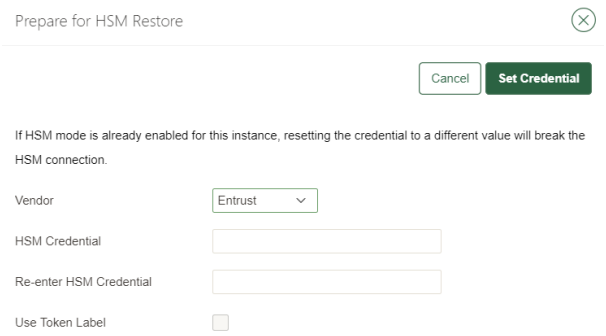
The **Token** label is **accelerator** if Module-Only protection is used (not required in this case).

Only the first two numbers of the firmware are included.

13. After a successful initialize operation of the nShield HSM, run the following command as the `oracle` user on the Key Vault server:

```
oracle$ /opt/nfast/bin/rfs-sync --commit
```

If you change the HSM credential on the HSM after initialization, you must also update the HSM credential on the Oracle Key Vault server: In the **Vendor** list, select **Entrust**, then select **Set Credential**.



2.4. Configure an HSM for a multi-master cluster

You can configure HSMs in a multi-master cluster with a single node or multiple nodes. In a multi-master Oracle Key Vault installation, any Key Vault node in the cluster can use any HSM. The nodes in the multi-master cluster can use different TDE wallet passwords (recovery passwords), RoT keys, and HSM credentials.

To ensure complete security, you must HSM-enable all Oracle Key Vault nodes in the cluster.

Entrust recommends that you read https://docs.oracle.com/en/database/oracle/key-vault/21.15/okvag/managing_multimaster.html for details on how to set up clusters.

This guide will set up the cluster from scratch. If you already have a cluster in place, read the documentation above.

To use an HSM within a cluster, start with a single node and add additional nodes as required.

There are two procedures for configuring an HSM in a multi-master cluster: starting with a single node or starting with multiple nodes. Both procedures are described in this guide, but Oracle recommends the single-node method.

2.4.1. Oracle recommendation to configure an HSM for a multi-master cluster starting with a single node

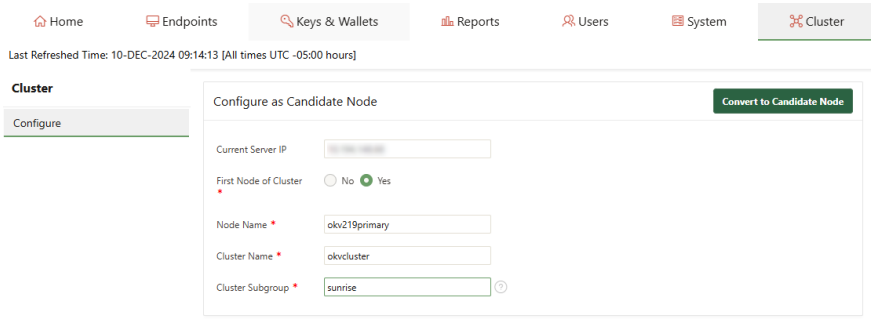
Oracle recommends the following steps to configure an HSM for a multi-master cluster starting with a single node:

1. Convert an Oracle Key Vault server into the first node of the cluster.
    a. Create the cluster by configuring the first node of the cluster.

b. Select the **Cluster** tab.

c. On the left menu, select **Configure**.

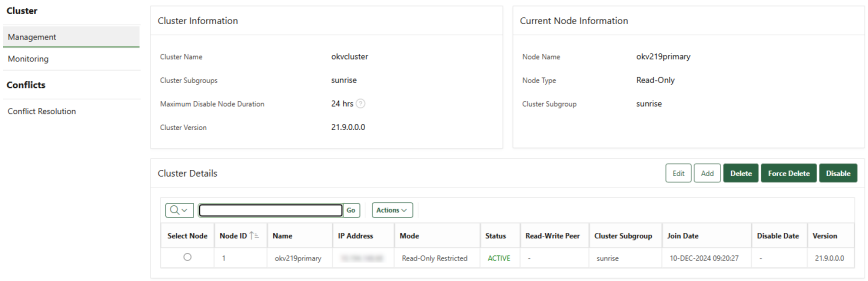
The **Configure as a Candidate Node** page appears. For example:



- For **Current Server IP**, enter the server IP address.
- For **First Node of Cluster**, select **Yes** if this is the first node, otherwise set it to **No**.
- **Node Name** is pre-populated with the host name of the OKV server.
- For **Cluster Name**, enter the name for the cluster.
- For **Cluster SubGroup**, enter the name of the group.

> If any node in the cluster is already HSM-enabled, you cannot add a new node that is not HSM-enabled.

d. Select **Convert Candidate Node**. The **Cluster Information** page appears.



2. HSM-enable the first node before adding any new nodes, see Enable HSM mode in Key Vault.
3. HSM-enable the candidate node before adding it to the cluster, see Enable HSM mode in Key Vault.
4. Add the HSM-enabled candidate node to the cluster using a controller node that is also HSM-enabled. Note the following:
   a. If any node in the cluster is already HSM-enabled, you cannot add a new node that is not HSM-enabled.

b. The Add Node to Cluster page on the controller node will require the controller node's HSM credential.

Refer to https://docs.oracle.com/en/database/oracle/key-vault/21.15/okvag/managing_multimaster.html for details on how to add a candidate node to the cluster.

2.4.2. Oracle recommendation to configure an HSM for a multi-master cluster with multiple nodes

Oracle recommends the following steps to configure an HSM for a multi-master cluster with multiple nodes:

1. Convert an Oracle Key Vault server into the first node (the controller node) of the cluster. The steps for this are described above.
2. Add the candidate nodes to the cluster using the controller node.

   Refer to https://docs.oracle.com/en/database/oracle/key-vault/21.15/okvag/managing_multimaster.html for details on how to add a candidate node to the cluster.

   After you create the initial node, you must add an additional read/write peer to the cluster.

   a. In the Controller Node, the one you just converted, select the **Cluster** tab, and then select **Management** from the left navigation bar.
   b. Under **Cluster Details**, select **Add**.
   c. In the **Add Candidate Node to Cluster** page, under **Add Cluster Details**, enter the recovery passphrase in the **Recovery Passphrase of the Cluster** field.

      This value will be used later when you pair with the candidate node. The recovery passphrase is that of the first node of the cluster and will be used later across all the cluster nodes.

   d. Enter the following details under Add Candidate Node Details.
      i. **Add Node as Read-Write Peer**: Select **Yes**.
      ii. **Node ID**: Select a unique ID for the candidate node. Remember that after you create this ID, you cannot change it. Node ID is auto populated but you may change it. Ensure that the candidate node ID is unique in the cluster.
      iii. **Node Name**: Enter a unique name of the candidate node. After you create this name, you cannot change it.
      iv. **Cluster Subgroup**: Enter the sub-group name for the candidate node. You can provide an existing subgroup name. If you provide a subgroup name that does not exist, it will be created. (This field is auto-populated with the cluster

subgroup name of the controller node.)

v. **Cluster Name**: Auto-populated and cannot be changed.

vi. **IP Address**: Enter the IP address of the candidate node.

vii. **Certificate of Candidate Node**: The next steps explain how you can find the certificate of the candidate node. (Do not exit this page.)

A. In a new browser window, log in to the Oracle Key Vault management console of the candidate node as a user who has the System Administrator role.

B. Select the **Cluster** tab, and then select **Configure** from the left navigation bar.

C. In the **Configure as Candidate Node** page, enter the following details:

I. **First Node of the Cluster**: Select **No**. Selecting No shows additional fields to enter.

II. **Recovery Passphrase of the Cluster**: Enter the recovery passphrase of the cluster that you entered earlier for the controller node.

III. **IP Address**: Enter the IP address of the controller node.

IV. **Certificate of Controller Node**: Use these steps to enter the certificate of the controller node:

1. In the browser window for the **controller node**, scroll to the bottom of the screen. Select and copy the entire certificate value shown for **Certificate of Controller Node**.
2. In the browser window for the **candidate node**, paste the copied certificate from the controller node into the **Certificate of Controller Node** field.
3. Check the recovery passphrase, the IP address, and the pasted in certificate very carefully to ensure that you copied it correctly. If there is an error, then after you click Convert to Candidate Node, you will need to terminate the pairing process or potentially reinstall Oracle Key Vault on this node.

viii. Click **Convert to Candidate Node**.

ix. The conversion can take several minutes. After the conversion is complete, the screen will refresh and the **Adding Candidate Node to Cluster** page is displayed. The certificate for the candidate node appears on this page.

x. Select and copy the entire candidate node certificate.

xi. In the browser window of the controller node, paste the copied certificate from the candidate node into the **Certificate of Candidate Node** field.

e. Click **Add Node**.

This process will take an hour or more, depending on the speed of your server, network, and volume of data in the cluster. During this time, the network management interface of the Oracle Key Vault will be restarted and you might momentarily get a Server Error 500 or the error Bad Gateway on the controller node. On the candidate node, errors may also appear, such as Bad Gateway. The candidate node will restart as part of the induction process. This is normal. During the pairing process, the status of the candidate node will display as PAIRING on all cluster nodes.

f. To view the status of any server, view the output on the management console.

After the candidate node restarts and completes the pairing process, you can log in to either cluster node to view the cluster status by selecting the Cluster tab. Ensure that the status of the new node shows as ACTIVE on all nodes in the cluster. The candidate node may briefly display that it is in read-only restricted mode after it automatically restarts. This node is now a synchronously paired cluster node and no longer a candidate node. After a node is part of a cluster, the console displays the node name, subgroup name, and cluster name in the top right area of the console header.

3. HSM-enable the controller node (first node).

Follow instructions to enable HSM mode on the first node of the cluster, see Enable HSM mode in Key Vault.

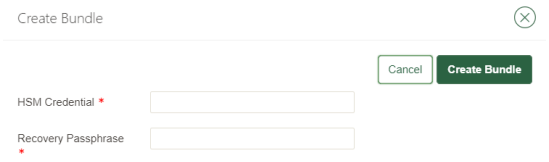
4. If multiple nodes are being used in the cluster, create an HSM bundle from the controller node and apply it to the candidate node(s).

You can configure HSM for the other nodes by copying information from the HSM-enabled controller node in the cluster. You do that by creating a bundle and applying the bundle to the candidate nodes in the cluster.

a. On the controller node of the cluster (first node), log in to the Oracle Key Vault web user interface as a Key Administrator.
b. Select the **System** tab.
c. On the left side of the **System** page, select **Settings**.
d. Under **Network Services**, select **HSM**. The **Hardware Security Module** page appears.

The controller node must be HSM enabled first.

e. Select **Create Bundle**.



f. Enter the HSM Credentials.

g. Enter the recovery passphrase.

h. Select **Create Bundle**.

A message indicating the bundle was created successfully appears.

i. Log in to the HSM-enabled controller node through SSH as the support user:

```
% ssh support@HSMENABLEDNODEIP
```

j. Copy the bundle to the candidate node using the node IP address:

```
% sudo scp /usr/local/okv/hsm/hsmbundle support@CANDIDATENODEIPADDRESS:/tmp
```

k. Log in to the candidate node in the cluster using its IP address:

```
% ssh support@CANDIDATENODEIPADDRESS
```

l. Perform the following steps to copy the bundle to the `/usr/local/okv/hsm` directory and apply user and group ownership:

```
% sudo cp /tmp/hsmbundle /usr/local/okv/hsm/
% sudo chown oracle:oinstall /usr/local/okv/hsm/hsmbundle
```

m. On the candidate node, select **Apply Bundle** on the **Hardware Security Module** page in the Web interface. Enter the recovery passphrase.

If you plan on reverse-migrating the original HSM-enabled node, you must apply the bundle immediately on all nodes first.

5. HSM-enable the candidate node.

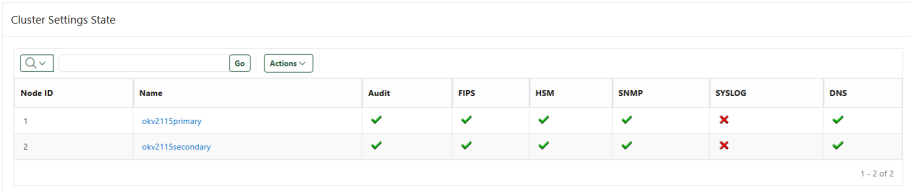
Follow instructions to enable HSM mode on the candidate node of the cluster when using multiple nodes, see Enable HSM mode in Key Vault.

6. Verify that each HSM is enabled in the cluster:

a. In the Oracle Key Vault web user interface, select the **Cluster** tab.

b. Select **Monitoring** in the left sidebar.

c. Check that the Cluster Settings State has all green ticks for HSM:



An enabled HSM does not mean that the HSM is active. The status only indicates whether the HSM is enabled for these nodes. To check whether the HSM is active, use the status information on the **Hardware Security Module** page of the web user interface.

The FIPS column is specific to Oracle Key Vault and does not indicate nShield HSM FIPS compliance. Entrust nShield HSMs are FIPS 140 Level 2 and 3 compliant.

7. After you have HSM-enabled all nodes and verified the replication between all nodes, remove the `hsmbundle` file from all of the nodes.

2.5. Reverse migration operations to a local wallet

Reverse migrating an HSM-enabled Oracle Key Vault server reverts the Key Vault server to using the recovery passphrase to protect the TDE wallet. This operation is necessary if the HSM that protects Oracle Key Vault must be decommissioned.

- Reverse migrating a standalone deployment

  You can reverse migrate a standalone deployment by using the Oracle Key Vault web user interface.

- Reverse migrating a multi-master cluster

  You can reverse migrate a multi-master cluster by using the Oracle Key Vault web user interface.

2.5.1. Reverse migrate a standalone deployment

You can reverse migrate a standalone deployment by using the Oracle Key Vault web user interface.

1. Log in to the Oracle Key Vault web user interface as a Key Administrator.

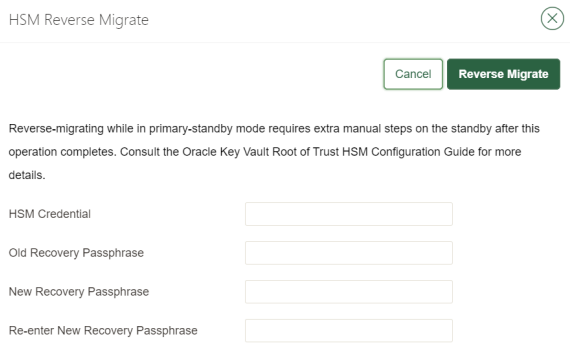
   The Oracle Key Vault **Home** page appears.

2. Select the **System** tab.

   The **Status** page appears.

3. On the left side of the **System** page, select **Settings**.
4. Under **Network Services**, select **HSM**.
5. Select **Reverse Migrate**.

   The **HSM Reverse Migrate** dialog box appears.



6. In the **HSM Reverse Migrate** dialog box, enter the following details:
   a. For **HSM Credential**, enter the HSM credential. For nShield HSMs, the credential is what you use for OCS, Softcard, or Module-Only protection.
   b. For **Old Recovery Passphrase**, enter the old recovery passphrase.
   c. For **New Recovery Passphrase**, enter the new recovery passphrase. Repeat this in **Re-enter New Recovery Passphrase**.
7. Select **Reverse Migrate**.
8. The **Hardware Security Module** page appears. The red downward arrow indicates the **Status**.

2.5.2. Reverse migrate a multi-master cluster

You can reverse migrate a multi-master cluster by using the Oracle Key Vault web user interface. This is required on each of the nodes in the cluster.

1. Log in to the Oracle Key Vault web user interface as a Key Administrator.

   The Oracle Key Vault **Home** page appears.

2. Select the **System** tab.

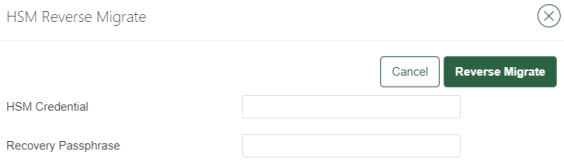
   The **Status** page appears.

3. On the left side of the **System** page, select **Settings**.
4. Under **Network Services**, select **HSM**.

   The **Hardware Security Module** page appears.

5. Select **Reverse Migrate**.

   The **HSM Reverse Migrate** dialog box appears.



6. In the **HSM Reverse Migrate** dialog box, enter the following details:
   a. For **HSM Credential**, enter the HSM credential. For nShield HSMs, the credential is what you use for OCS, Softcard, or Module-Only protection.
   b. For **Old Recovery Passphrase**, enter the old recovery passphrase.
   c. For **New Recovery Passphrase**, enter the new recovery passphrase. Repeat this in **Re-enter New Recovery Passphrase**.
7. Select **Reverse Migrate**.

   The **Hardware Security Module** page appears. The red downward arrow indicates the **Status**.

2.6. Configure backup of the Key Vault server in HSM mode

To configure backup of the Key Vault server in HSM mode:

1. Log in to the Oracle Key Vault web user interface as a Key Administrator.

   The Oracle Key Vault **Home** page appears.

2. Select the **System** tab.

   The **Status** page appears.

3. On the left side of the **System** page, select **Settings**.

4. Under the **System Configuration**, select **Backup and Restore**.
5. Add the backup destination on the **System Backup** page, just as you would in non-HSM mode.
6. Perform a backup as usual from the web user interface.

2.7. Restore from a Key Vault backup in HSM mode

To restart or restore Key Vault in HSM mode when OCS protection is used, the OCS for the HSM must be in slot 0 of the HSM.

Only backups taken in HSM mode can be restored onto an HSM-enabled Oracle Key Vault. Before you restore a backup onto a system, you must ensure that the system can access both the HSM and the Root of Trust used to take the backup. You must therefore have installed the HSM on the Oracle Key Vault server and enrolled Oracle Key Vault as a client of the HSM prior to this step.

1. If OCS protection is used, present the OCS card to the HSM.
2. Log in to the Oracle Key Vault web user interface as a user with system administrative privileges.

   The **Oracle Key Vault Home** page appears.

3. Select the **System** tab.

   The **Status** page appears.

4. On the left side of the **System** page, select **Settings**.
5. Under **Network Services**, select **HSM**.

   The **Hardware Security Module** page appears. On restore, the **Status** is disabled first, then enabled after the restore completes.

6. Select **Set Credential**.

   The **Prepare for HSM Restore** screen appears.

7. From the **Vendor** list, select **Entrust** and enter the HSM credential twice as requested.
8. Select **Set Credential**.

   The HSM credential will be stored in the system. This HSM credential must be entered manually to do an HSM restore because it is not stored in the backup itself.

9. On the left side of the page, select **Settings**.

10. Under the **System Configuration**, select **Backup and Restore**.
11. Select **Restore** and restore the Key Vault backup.

2.8. Restart or restore in HSM mode using nShield Remote Administration

To restart or restore Key Vault in HSM mode when OCS protection is used, the OCS for the HSM must be in slot 0 of the HSM.

The `raserv` package of nShield software is available only on the nShield RFS machine; it is not supported on Oracle Key Vault servers. When the Oracle Key Vault server restarts or restores from a backup and Java Cards cannot be presented to the HSMs that are enrolled to that server, the restart or restore will fail.

If the HSM is also enrolled to the RFS, you can present Java Cards there when the RFS is operational. As a result, when the Oracle Key Vault server comes back up, it can still access the keys from the HSM using the OCS in slot 0.

Chapter 3. Additional resources and related products

3.1. nShield HSMs

3.2. nShield as a Service

3.3. Entrust products

3.4. nShield product documentation